UDC 621.391.3

SECURITY ISSUES THAT WILL DOMINATE IN IOT NEAREST FUTURE

Minochkin D. A., Radchuk A.V.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: radchyk9696@gmail.com

Питання безпеки, які домінуватимуть у найближчому майбутньому в IoT

The Internet of Things (IoT) will face multiple threats over the next few years. Due to Given large amount of private information, providing information security on the shared data is an important issue that cannot be neglected. In this article, we present with general information about the topics related to new DNS issue, insufficient certification in public-key and cryptosystems.

The main challenge of object identification is to ensure the integrity of records used in the naming architecture. Although the Domain Name System (DNS) provides name translation services to Internet users, it is an insecure naming system. It remains vulnerable to various attacks, such as DNS cache poisoning attack, and man-in-the-middle attack. This poisoning attack injects counterfeit DNS records into victims' cache and directly compromises the resolution mapping between naming architecture and addressing architecture. Therefore, without the integrity protection of the records, the entire naming architecture is insecure. Domain Name Service Security Extension (DNSSEC, IETF RFC4033) is deployed as the security extensions of DNS. DNSSEC can ensure the integrity and authenticity of a Resource Record (RR), and at the same time serve as a vehicle for the distribution of cryptographic public keys. Although DNSSEC seems to be a remedy for naming services, it is still challenging to deploy DNSSEC properly in IoT. DNSSEC incurs high computation and communication overhead and may not be suitable for IoT devices. A new naming service is desirable [1].

Although public-key cryptosystems have advantage for constructing authentication schemes or authorization systems, the lack of a global root certificate authority (global root CA) hinders many theoretically feasible schemes from actually being deployed. Without the global root CA, it becomes very challenging to design an authentication system for IoT. Furthermore, it may be infeasible to issue a certificate to an object in IoT since the total number of objects is often huge. Therefore, the concept of delegated authentication and delegated authorization must be taken into consideration for IoT [1].

Wearable gadgets take measurement and report it to mobile APPs. These collected data are then passed on to smart furniture and/or appliance in smart home/office to make adjustment accordingly. This is a common IoT application demonstrated in CES 2015. [2] The communication scenario of information exchange can be broken into two categories according to the distance range, that is, domestic and foreign. Typical domestic communication is done locally without access to the public network (a.k.a. the Internet). Foreign communication, on the other hand, relies on the public network to distribute data to distant objects.

Heterogeneity of objects is expected in IoT where objects have limited resources, computing power and communication capability. With the nature of lightweight and portability, the communication capability of wearable devices is mostly in a short distance. Short-range wireless communication (i.e. domestic communication), such as Bluetooth, relies on pairing objects prior to data exchange.

For wearable devices to extend the communication range (i.e. foreign communication), a delegator is required to relay the data traffic. Delegator is normally referred to as the gateway of communication. For wearable devices made for mobility, the handheld device such as mobile phone is a suitable gateway to relay data. On the other hand, for home/office appliances, a hotspot such as wireless AP (Access Point) is a suitable candidate to relay data. Figure 1 [3] illustrates the typical topology configuration for both long distance and short distance communication. For domestic communication authentication, e.g. Bluetooth, basic security is provided in the link layer during object pairing where password is required. Once the object is paired, encryption is applied when data has been exchanged wirelessly. On the other hand, foreign communication authentication, will enumerate a number of applicable authentication models.

Since IoT comes at a massive scale of objects, naming of the objects becomes more complex. Due to the heterogeneity of the objects and the network, conventional Internet naming and identification will not be applicable. Uniquely naming the objects is one of the main challenges in IoT to be resolved before addressing object authentication. GS1 suggested that the DNS naming scheme can be the naming basis of IoT given that IoT is to be deployed on the Internet. Object Naming Service (ONS) is part of GS1 EPCglobal architecture framework [2] that leverages DNS to locate authoritative metadata and services with given Electronic Product Code (EPC). The

EPC is designed for the purpose of providing universal unique identity. ONS can also be integrated into DNS as a sub-domain of DNS. Therefore, the Internet becomes the communication medium for the devicenaming domains.

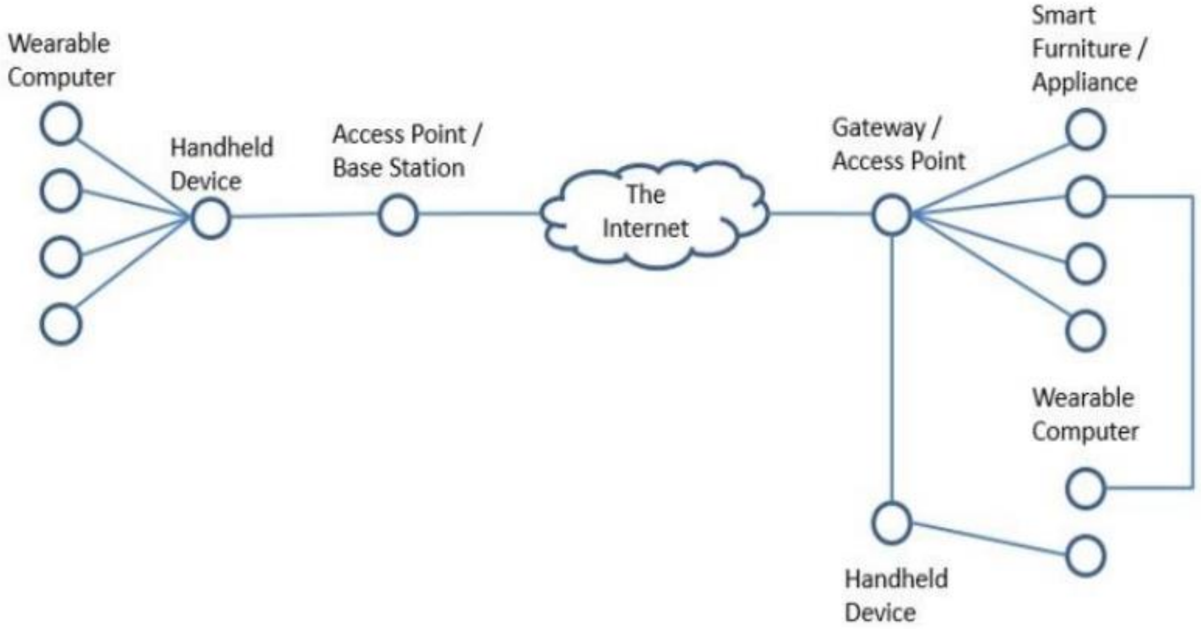

Fig. 1. A typical IoT topology [3].

As an illustrator of the future Internet architecture, US NSF launched Future Internet Architecture Project (FIA Project). As a core sub-project of FIA Project, L. Zhang et al. proposed novel "Named Data Networking (NDN)" [3] which moves the network architecture from host-centric to data-centric. According to NDN, the identification and network routing are based on the name of the object instead of using conventional IP address. Naming in NDN is in a hierarchical structure, and is applicable to hierarchical nature of the current computer network structures. NDN has great impact, but is still in its infancy. There are still many new challenges, such as efficiency, name validation, signing key management, object authentication, and other security issues. These challenges remain unsolved and raise concerns.

In this part, we will depict the challenges to IoT deployment on preserving privacy. The challenges can be divided into two categories: data collection policy and data anonymization. Data collection policy describes the policy during data collection where it enforces the type of collectable data and the access control of a “Thing” to the data. Through the data collection policy, the type and amount of information to be collected is restricted in the data collection phase. Since the collection and storage of private information is restricted, privacy preservation can be ensured. The second challenge is data anonymization. To ensure data anonymity, both cryptographic protection and concealment of data relations are desirable. Given the diversity of the "Things", different cryptographic schemes may be adopted. For example, lightweight cryptographic schemes are more suitable to devices that have resource-constraints. The second category, concealment of data relation, investigates the removal of direct relations between the data and its owner. This also can be achieved by applying data encryption where scrambled data have resistance against data analysis. However, information needs to be shared amongst "Things" in IoT; therefore, computation on encrypted data is another challenge for data anonymization. To cope with the problem, some of research works in homomorphic encryption may be applicable.

Lightweight Cryptosystems and Security Protocols. Compared with symmetric-key cryptosystems, public-key cryptosystems generally provide more security features but suffer from high computational overhead. However, public-key cryptosystems are often desirable when data integrity and authenticity are needed. Therefore, computation overhead reduction for public-key cryptosystems as well as complex security protocols remains a major challenge for IoT security. [1]

CONCLUSION. The main features that differentiate IoT security issues from the traditional ones are the heterogeneous and large-scale objects and networks. These two factors, heterogeneity and complexity, make IoT security much more difficult to deal with. This article is aimed at ongoing challenges and research opportunities in IoT security. New research topics and their possible solutions are also discussed.

References

1. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities", 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, (DOI: 10.1109/SOCA.2014.58), 17-19 Nov. 2014, p.5.

2. Zhi-Kai Zhang, Michael Cheng Yi Cho, Shiuhpyng Shieh "Emerging Security Threats and Countermeasures in IoT ". Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security Feb. 2015, Pages 1-6.

3. Mung Chiang "Fog and IoT: An Overview of Research Opportunities", IEEE Internet of Things Journal, Volume: 3, Issue: 6, Dec. 2016, pp. 854 – 864.